Keywords: software authorization, piracy, theft prevention, software lock, dongle, iButton, iButton security Apr 27, 1999

APPLICATION NOTE 97

Features, Advantages, and Benefits of Button-Based Security

This document describes the features, advantages, and benefits of Button-Based Security in regards to software authorization. Some of the benefits discussed include: unique identification, automatic registration, audit control, security, passwords, hierarchical security, enabling encryption, and introducing software metering.

Uniquely Identifiable

Each Button contains a unique and unalterable 64-bit identification number that is lasered into each silicon chip contained inside the Button's tamperproof case. The identification number can be used for registration, audit and security purposes.

Automatic Registration
The serial number can be used as a registration number for each software package sold. The Button ID is read into a database and is associated with a customer number or invoice. Product options purchased can also be recorded. This process can be automated.

Audit Control
Once deployed, Button identification numbers can act as an audit trail. This is useful when resolving billing disputes, or for engineers troubleshooting problems.

Security
Use the serial number as a seed to generate a password. This allows you to vary passwords for each copy distributed while avoiding manual insertion of a unique password.

Read/Write Devices

Buttons are devices which can be read and written to. Changes are made to Button memory areas even as the software application is being executed by the customer. This feature is vital to creating dynamic security schemes. Read/write capability is also useful for version control, tracking software usage, and storing statistics.

Programmable Passwords
DS1425 Buttons allow you to program your own passwords. Independent passwords can be set for each of the three DS1425 RAM pages. Circuitry inside the Button will match future passwords with this register. Only you then hold the key to opening the Button, for only you know the password.

In contrast, conventional protection devices will assign you a family code number which the manufacturer controls. This scheme has two weaknesses. First, you don't control it, you rely on some entity outside your company to ensure security is not broken. Secondly, your entire security scheme is defeated if the family code is exposed.

The Dallas scheme eliminates these weaknesses. First you program the passwords, giving you control. Second, by choosing different passwords for each application (and even each customer), a compromise in security would only affect one Button and one customer, not the entire security scheme.

False passwords written to the DS1425 will automatically invoke a random number generator (contained in the Button) that replies with false responses. This eliminates attempts to break security by pattern association. Conventional protection devices do not support this feature.

Generate Unique Passwords for Each Button
The Button serial number can be used to build unique passwords, providing a unique security code for each copy of the software distributed. Choose an algorithm and use the unique serial number as a seed, allowing each Button to have a different password. The algorithm and serial number eliminates the need to customize each software package to a particular Button, or have the same password for all Buttons. Different passwords can be spread across customers achieving very high security.

For example, application software could read a Button serial number, and exclusive OR it with another seed number stored in the application. The result is a unique password that must be matched with the preset password in the DS1425's write only registers.

No Special Programming Hardware Required
Buttons (with the exception of the DS1422) do not require any special hardware interface for programming. The Button Holders can read and write to the Buttons. Changes to the contents of the Button memory can be made before or after the release of the software (at a customer site while the application is executing).

Dynamic Passwords
The password that secures the data in the Button can be changed at any time by the application. Note that changing the password always requires the knowledge of the old password to perform the change.

Buttons modifications can be made in the field during the operation or installation of your software, transparently. For example, the installation process of new software options recently purchased could include routines that register the new options (inside the Button) and set a new password. Password changes can also be made at the end of every user session.

Hierarchical Security
The DS1425 Multi-key Button contains three separate, independently password-protected memory storage areas. Each password is eight bytes.

For advanced security applications, the three memory areas can all be used to protect one application. If information critical to operating the application is stored in page three (and password protected), its password could be stored in page two. In like fashion, storage area two's password could be stored in storage area one and locked using its passwords. The net effect is a "nesting" of passwords which provides three levels of protection.

Enabling Encryption
Buttons can also act as storage devices for encryption information. Algorithms, keys, and seeds can all be stored and password protected. Password protecting decryption keys is particularly useful for implementing specific authentication (and subsequent audit logging) mechanisms for individual encryption/decryption sessions. Storing keys in the Button also eliminates the need for users to know (and remember) their key, and enforces possession of the Button to perform the transaction. Possession and the elimination of knowledge may be highly desirable, as it raises the overall security of the encryption scheme and makes it easier to use.

Machine Independence

Button communication is based on a standard protocol that is independent of any platform or operating system. Buttons operate with different platforms without any changes.

Common Authorization Model Across All Platforms

The portable nature of the Button streamlines license authentication across platforms. For example, by removing a Button from a holder on computer A and placing it in the Button Holder of computer B, a customer can effectively transfer a fixed license without your involvement. You still maintain control, because the software stored on Computer A (without a Button) will not operate.

Buttons operate independently from specific hardware or operating systems, which allows for a common license scheme across multiple platforms. Simple license schemes can be easily implemented and maintained as platform support for the application grows.

Machine independence also promotes the concept of personalized licenses. By programming the individual access rights of each user into each of their Buttons, and distributing them on a per user basis, their "right to use" the software is carried with them as they travel, allowing them to use your software from any access point. Possession of a Button is the key to gaining access and controlling use.

Reduce Update Overhead
Sending out demos, upgrades or new releases only requires a new Button. The holder is reusable. Buttons can be replaced with the same or other Button types that contain new password or secured product information.

The Buttons also are re-usable; knowing the correct password allows memory to be changed. In this sense, Buttons can be updated remotely (through the installation process of the update) transparent to the user. This action automatically allows the license governed by the Button to be transferred from the old version to the new, and disables the operation of the old version (since the Button contents has changed).

Eliminates Hardware Lock Incompatibilities
Button based software protection schemes eliminate incompatibilities caused by having different vendor "dongles" stacked on the end of user machines. A standardized 1-wire interface allows multiple Buttons to be connected together using a single holder on a computer's I/O port. Each software vendor can issue a Button to secure their software package and be assured that their protection device is compatible with the existing ones.

CD ROM Distribution

Button based schemes enhance the distribution process for software vendors choosing to use CD-ROM as a media. This is accomplished using similar schemes to floppy disk distribution, maintaining consistency across media, with virtually no extra cost.

Using the DS1425 Multi-Key Button, a product matrix of software suites that are distributed on the CD-ROM can be protected. The licenses for the applications of the CD-ROM are enabled through the Buttons product matrix. Initial pre-settings can be made (according to the original customer order) and changed using extensions to the dynamic password schemes discussed earlier.

For advanced CD-ROM distribution applications, the DS1427 Time Button can operate in conjunction with the DS1425 to mix temporary and permanent licenses. This is most beneficial when customers purchase portions of the CD-ROM' s contents and later desires evaluations of other portions.

The Button based system is particularly elegant for CD- ROMs because it allows execution control across all applications of the media, yet is easily changed. These features are consistent with the reason CD-ROMs are used for distribution, controlled exposure to software suites.

Product Upgrades
CD-ROM based application licenses can be updated in two ways. One, the vendor may choose to program and issue a new "update" Button. At the customer site, the update Button is used to transfer the new license information into the original Button. The update Button is subsequently disabled.

The second method is to store all the password information in the product matrix initially, and issue individual passwords by phone, fax, or mail, to enable individual applications after distribution. This method does not require the use of additional Buttons.

Secure Distribution
The unique serial number of each Button can be used to prevent customers from mixing Buttons and extending licenses. Enabling passwords for each application can be built using an algorithm which is seeded by each CD-ROM's and/or Button's serial number, tying the passwords to an individual distribution. Using the serial number of a DS1427 Time Button ties a real-time clock to the same distribution, further extending this level of execution control to temporary licenses.

The Quality of Dallas Semiconductor

No "dongle" manufacturer can boast equivalent quality to the Buttons. Dallas is the only semiconductor manufacturer that markets software protection devices.

Dallas applies the same rigorous quality standards to its Software Authorization products that it does to its integrated circuits. We measure our failure rates in parts per million, and our MTBF (mean time between failures) in decades. Dallas spends millions of dollars each year to ensure that every product manufactured passes world class quality standards.

Buying from Dallas allows you to take advantage of the same quality your customers do, since our real time clock chip is probably installed in their PC.

Introduce Metering into your License Scheme

The DS1427 Time Button contains a tamperproof realtime clock. Using this Button allows you to control the usage of your software by time. During the pre-sales process, time limited evaluations of your full suite of software can be deployed, eliminating the cost of maintaining demonstration versions, and reducing the overhead of converting an evaluator to a customer. Conversion means removing the DS1427 and replacing it with a DS1425.

Since the DS1427 has an ID, it too is traceable, so that you can maintain an audit trail of the demonstrations and evaluations that are being performed. This traceability can allow your outside sales or telemarketing resources to follow up using a data base. Time metering also allows you to respond to peak customer demands for your software, eliminating the overhead of expedition and key management. By issuing the Time Button, customers can make copies of your software, and use them for a controlled time period. When the time expires, those same copies are not executable. Therefore, the total overhead to respond to a short term demand is reduced to issuing one or a group of Buttons.

The DS1427 also contains an expiration alarm and 512 bytes of RAM. Once set, the alarm can be used to expire the Button making it unusable to anyone. This absolute lockout feature is beneficial for product evaluations. If not purchased, the software application can never be used again.

The developer can also place encrypted passwords in the RAM space of the Button. These passwords can be used to re-enable time periods to extend the evaluation or rental of the software. The customer simply calls in and receives a password to re-enable the software for a given time period, say 60 days.

The software matches the password with a preset valid encrypted time period stored in the Button's RAM. The time period is determined by calculating a timeout date and time based on the Button's real-time clock. The timeout date and time is then stored in the Button RAM. When the application needs time validation, it retrieves the timeout date and time from the RAM in the Button and compares it to the value of the real-time clock. If the date and time of the real time clock is beyond the timeout date and time, access is denied.

Compatible with Emerging Standards

Never before has it been more important to comply with standards. Dallas Semiconductor is working with many of the leading software and hardware companies to ensure that Button based copy protection is compatible with all the appropriate standards.

Two emerging standards are most important when considering protection devices today. Compatibility with future licensing standards and compatibility with PC security.

License Management Servers
Many of the network operating system vendors have already incorporated network license managers into their next generation products. As these new products become available, license servers will allow you to manage the distribution of your network software with a tool that is tightly coupled to the operating system.

Buttons have been unanimously selected as the technology of choice by license management providers. Now you will be able to take advantage of Button protection and license management in a seamless fashion.

Button Ready Computers
Distributed computers (and personal computers in particular) have for a long time suffered from the lack of adequate resources to build security applications upon. This fact is the very reason why external protection devices exist.

However, the Button technology represents the first opportunity to introduce security into the distributed computer. Why ? Because the security is in the Button, not in the dongle. The external connector, which in the Dallas scheme is not much more than a facilitator of communications between the Button and the CPU, **can be eliminated**.

The massive reduction in communication complexity, coupled with Dallas' ability to fabricate semiconductor devices, and our vast knowledge of distributed computers, have all been harnessed to bring you computers that are equipped with Button Holders. These computers accept Buttons directly, eliminating the need for external connectors, and reducing protection costs to the price of the Button.

In essence, a new port has been created that is dedicated to security and makes copy protection affordable to all software vendors. This new resource is also a new foundation from which software vendors can create new and better security applications.

Only the Dallas Button scheme is compatible with this new port, and choosing Buttons today ensures compatibility.

Application Note 97: http://www.maxim-ic.com/an97

More Information
For technical questions and support: http://www.maxim-ic.com/support
For samples: http://www.maxim-ic.com/samples
Other questions and comments: http://www.maxim-ic.com/contact

Related Parts

DS1410E:	QuickView	-- Full (PDF) Data Sheet
DS1425:	QuickView	-- Full (PDF) Data Sheet
DS1427:	QuickView	-- Full (PDF) Data Sheet

DS1991: QuickView -- Full (PDF) Data Sheet -- Free Samples

DS1994: QuickView -- Full (PDF) Data Sheet -- Free Samples

AN97, AN 97, APP97, Appnote97, Appnote 97